Nathan R. Ring
STRANCH, JENNINGS & GARVEY, PLLC.
Nevada State Bar No. 12078
3100 W. Charleston Blvd., Ste. 208
Las Vegas, Nevada 89102
(725) 235-9750
nring@stranchlaw.com

Raina C. Borrelli, Esq.*
Samuel J. Strauss, Esq*
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Phone: (872) 263-1100
Fax: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

Attorney for Plaintiff Josephine Russo

IN THE UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

JOSEPHINE RUSSO, individually and on behalf of all others similarly situated, Plaintiff, v. EFFORTLESS OFFICE ENTERPRISES, LLC, Defendants.	Case No.: **PROPOSED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

PROPOSED CLASS ACTION COMPLAINT

Plaintiff, JOSEPHINE RUSSO ("Plaintiff"), on behalf of herself and all others similarly situated, states as follows in her Class Action Complaint against Defendant EFFORTLESS OFFICE ENTERPRISES, LLC ("EOE" or "Defendant"):

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

INTRODUCTION

1. For an astonishing 75 days, from May 9, 2024 to July 23, 2024 Defendant lost control over its computer network and the highly sensitive personal information stored therein in a data breach perpetuated by cybercriminals ("Data Breach"). On information and belief, the Data Breach has impacted Defendant's clients' current and former customers.

2. The Data Breach resulted in unauthorized disclosure, exfiltration, theft, and dissemination on the dark web of Defendant's clients' current and former customers' highly personal information, including, on information and belief, names, Social Security numbers, driver's license or other government-issued ID numbers, financial information ("personally identifying information" or "PII"), and medical information and health insurance information ("protected health information" or "PHI"). Plaintiff refers to both PII and PHI collectively as "Sensitive Information."

3. EOE's Data Breach affects current and former customers of Defendant's clients who had no relationship with EOE, never sought one, and never consented to EOE collecting and storing their information.

4. EOE sourced their information from third parties, stored it on its systems, and assumed a duty to protect it, despite advertising that it delivers "secure cloud products and services."[1] But EOE never properly implemented the security safeguards it promised despite acknowledging their importance.

5. On information and belief, the Data Breach occurred from May 9, 2024 to July 23, 2024. Due to the obfuscating language in the notice letter EOE sent to victims of the Data Breach (the "Breach Notice")[2] it is unknown how the Data Breach happened, when EOE became aware it

---

[1] *About Effortless*, EOE, https://effortlessoffice.com/about/ (last visited June 25, 2025).

[2] A sample Breach Notice is attached hereto as **Exhibit A**.

had been hacked by cybercriminals, or why cybercriminals had free reign over Defendant's IT environment for 75 days. EOE eventually notified Plaintiff and the Class about the Data Breach on June 13, 2025, *339 days* after the Data Breach occurred.

6. At this it is unknown how many individuals were affected by the Data Breach. However, a known cybercriminal group, Blacksuit, has taken credit for the Data Breach on its dark web "data leak site."[3]

7. Accordingly, Plaintiff and the Class had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of their privacy from having their Sensitive Information disseminated on the dark web and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

8. Due to its lack of direct notice about the Data Breach to the Class, EOE has obfuscated the nature of the breach and the threat it posted—refusing to tell breach victims how the breach happened, or why it took EOE 339 days to notify victims that hackers had stolen its clients' highly private Sensitive Information.

9. Defendant's failure to timely detect and report the Data Breach made breach victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Sensitive Information.

10. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of misuse of their Sensitive Information.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

[3] Falcon Feeds (@FalconFeeds.io), X (Aug. 31, 2024 4:20 PM), https://x.com/FalconFeedsio/status/1829992740509401154.

11. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class (or their third party agents) trusted Defendant with their Sensitive Information. But Defendant betrayed that trust. Defendant failed to effectively use up-to-date security practices to prevent the Data Breach.

12. Plaintiff Josephine Russo is a Data Breach victim.

13. Accordingly, Plaintiff, on her own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

14. The exposure of one's Sensitive Information to cybercriminals is a bell that cannot be unrung. Before this data breach, Defendant's clients' current and former customers' private information was exactly that—private. Not anymore. Now, the Class's Sensitive Information is forever exposed and unsecure.

PARTIES

15. Plaintiff Josephine Russo, is a natural person and citizen of Nevada, residing in Henderson, Nevada, where she intends to remain. Plaintiff is a Data Breach victim, having received a Breach Notice from Defendant.

16. Defendant, Defendant Effortless Office Enterprises, LLC is a limited liability company organized under Nevada law and with its principal place of business located at 3130 S Rainbow Blvd, SUITE 303, Las Vegas, NV, 89146

JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because the amount in controversy exceeds $5 million (exclusive of interest and

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

costs), at least one Class Member and Defendant are citizens of different states, and because there are over 100 putative Class members.

18. Many states, including California and Texas, have statutes requiring companies to report data breaches to the relevant state's attorney general's office. *See* Cal. Civ. Code § 1798.82; Tex. Bus. & Com. Code Ann. § 521.053.

19. Pursuant to Cal. Civ. Code § 1798.82, Defendant submitted a letter and other information about the Data Breach to the affecting California citizens to California Attorney General's Office, which is publicly available.[4]

20. Pursuant to Tex. Bus. & Com. Code Ann. § 521.053, Defendant submitted information about the Data Breach affecting Texas citizens to the Attorney General of Texas, which is publicly available.[5]

21. Because Defendant has publicly reported the existence of members of the proposed class in California and Texas, Plaintiff has satisfied the minimal jurisdictional requirements set forth in 28 U.S.C. § 1332(d)(2) in that there are many members of the putative class who are citizens of states different from Defendant.

22. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District and does substantial business in this District.

23. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

---

[4] *Submitted Breach Notification Sample*, STATE OF CALIFORNIA DEPARTMENT OF JUSTICE, https://oag.ca.gov/ecrime/databreach/reports/sb24-604038 (last visited June 25, 2025).

[5] *Data Security Breach Reports*, ATTORNEY GENERAL OF TEXAS, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited June 25, 2025).

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

STATEMENT OF FACTS

EOE

24. EOE states it is a "Hybrid Managed Services Provider that delivers and fully supports secure cloud products and services giving customers a single solution provider for entire IT environments."[6]

25. EOE also claims that it "delivers proactive cybersecurity solutions that protect your organization from the most sophisticated attacks" and that its "services are designed to safeguard your critical data, systems, and networks with a multilayered defense strategy."[7]

26. As part of its business, Defendant receives and maintains the Sensitive Information of thousands of its clients' current and former customers. In collecting and maintaining the Sensitive Information, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class members themselves took reasonable steps to secure their Sensitive Information.

27. Indeed, in its Privacy Policy, under the heading "How do we protect your personal data," EOE boasts:

> At Effortless Office, we recognize that privacy is critical in today's digital environment. We are committed to safeguarding the personal information of our clients, partners, and website visitors. Our privacy practices are designed to meet the highest standards of data protection and security, ensuring your information is handled with care and respect. We are SOC 2 Type 2 certified, reflecting our

---

[6] *Effortless Office*, LINKEDIN, https://www.linkedin.com/company/effortless-office/about/ (last visited June 25, 2025).

[7] *EFFORTLESS Cybersecurity*, EOE, https://effortlessoffice.com/services/cybersecurity/ (last visited June 25, 2025).

dedication to maintaining robust security, availability, and confidentiality of the data we process.[8]

28. Despite recognizing its duty to do so, on information and belief, EOE has not implemented reasonable cybersecurity safeguards or policies to protect its client's Sensitive Information or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, EOE leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' Sensitive Information.

The Data Breach

29. On information and belief, Plaintiff provided her Sensitive Information to a client of Defendant.

30. On information and belief, Defendant collects and maintains its clients' current and former customers' Sensitive Information in its computer systems.

31. In collecting and maintaining Sensitive Information, Defendant implicitly agrees that it will safeguard the data using reasonable means according to its internal policies, as well as state and federal law.

32. According to Defendant's Breach Notice, EOE "discovered suspicious activity temporarily within its computer network" and "promptly took steps to secure the environment and began an investigation."[9]

33. EOE states that its "investigation determined that unauthorized access occurred at certain times between May 9, 2024 and July 23, 2024" and it "completed a comprehensive

[8] *Privacy Policy of Effortless Office*, EOE, https://effortlessoffice.com/privacy-policy/ (last visited June 25, 2025).
[9] Ex. A.

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

programmatic and manual review to identify what personal information was impacted."[10] According to EOE, this investigation concluded on May 12, 2025.[11]

34. Thus, due to Defendant's lack of oversight and technical safeguards over its IT environment, cybercriminals were permitted to roam free in its computer network for *75 days*

35. And yet, Defendant waited over until June 13, 2025, a month after its investigation purportedly concluded, before it began notifying the class.[12]

36. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

37. And when Defendant did notify Plaintiff and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiff and the Class to "review your current and past credit and debit card account statements for discrepancies or unusual activity."[13]

38. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information. This is especially true here, as Defendant claims to provide cybersecurity services that "protect your organization from the most sophisticated attacks."[14] Defendant's failure to implement the very cybersecurity it claims to provide caused widespread injury and monetary damages.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

---

[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] N. 7.

39. Since the breach, Defendant has declared that it has "implemented additional measures to enhance the security of its network environment."[15]

40. However, mere claims of "additional measures" do not establish that Defendant ***actually enhanced*** its data security to a sufficient level. Thus, injunctive relief is necessary to ensure that Defendant institutes adequate data security to protect the Sensitive Information that it still retains.

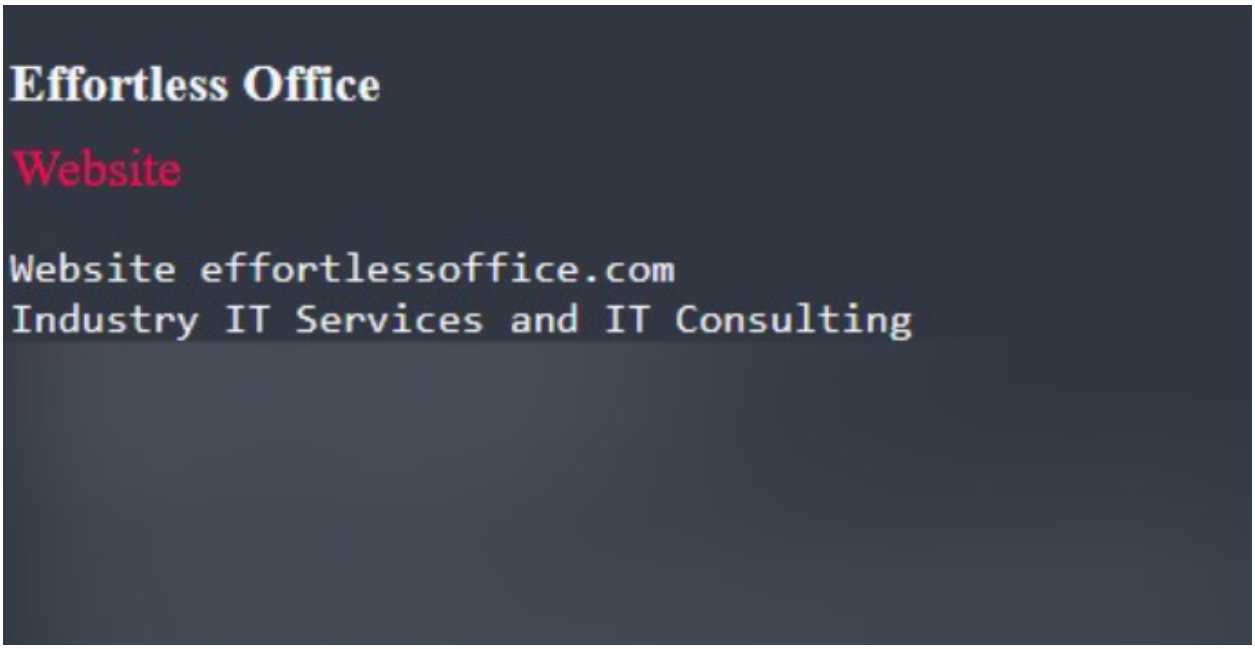
41. Defendant has done little to remedy its Data Breach. True, Defendant has offered Data Breach victims credit monitoring and identity related services. But upon information and belief, such services are wholly insufficient to compensate Plaintiff and Class members for the injuries that Defendant inflicted upon them.

42. Because of Defendant's Data Breach, the Sensitive Information of Plaintiff and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon them.

[15] Ex. A.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

43. As Defendant conducted its ten month investigation, on August 31, 2024, the ransomware group Blacksuit claimed responsibility for the Data Breach on its dark web portal.[16]



44. According to the Cybersecurity and Infrastructure Security Agency ("CISA") Blacksuit steals and then encrypts files and engages in double extortion tactics, threatening to publicly release organizations' exfiltrated data if it does not pay a ransom.[17] CISA further warns that Blacksuit uses a leak site to publish victim data based on non-payment.[18]

45. Thus, on information and belief, Plaintiff's and the Class's Sensitive Information has already been published, or will be published imminently, on the dark web.

46. In its Breach Notice, EOE did not inform Data Breach victims that their Sensitive Information had been stolen by Blacksuit and published on the dark web..

---

[16] N. 3.
[17] *#StopRansomware: Blacksuit (Royal) Ransomware*, CISA (Aug. 27, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a.
[18] *Id.*

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

47. To date, EOE has made no public statements regarding Blacksuit or whether it paid a ransom demand.

48. However, even if Defendant made a ransom payment, there is no guarantee that the data Blacksuit stole will be deleted.[19] The stolen Sensitive Information is valuable, and can easily be sold to another threat actor, so there is little incentive to delete it.[20]

49. Defendant failed to notify the Class, for *339 days*—depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

50. Despite its duties and alleged commitments to safeguard Sensitive Information, Defendant did not in fact follow industry standard practices in securing its clients' current and former customers' Sensitive Information, as evidenced by the Data Breach.

51. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's Sensitive Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

52. Due to the circulation of their Sensitive Information on the dark web, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' Sensitive Information is substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

---

[19] Steve Adler, *Majority of Ransomware Victims That Pay a Ransom Suffer a Second Attack*, THE HIPAA JOURNAL (Feb. 23, 2024), https://www.hipaajournal.com/majority-of-ransomware-victims-that-pay-a-ransom-suffer-a-second-attack/.

[20] *Id*.

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

53. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its clients' current and former customers' Sensitive Information. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

54. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare and healthcare adjacent industry preceding the date of the breach.

55. In light of recent high profile data breaches at other healthcare partner and provider companies, Defendant knew or should have known that its electronic records and consumers' Sensitive Information would be targeted by cybercriminals.

56. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.21 The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.22

57. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets

---

[21] *2021 Data Breach Annual Report*, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf (last visited June 25, 2025).

[22] *Id.*

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."23

58. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."24

59. In September 2020, CISA Agency published a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."25

60. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

61. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted Private Information of thousands

---

[23] *High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations*, FBI (Oct. 2, 2019), https://www.ic3.gov/Media/Y2019/PSA191002.

[24] Catalin Cimpanu, *Ransomware mentioned in 1,000+ SEC filings over the past year*, ZDNET (Apr. 30, 2020), https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/.

[25] *#StopRansomware Guide*, U.S. CISA, https://www.cisa.gov/stopransomware/ransomware-guide (last visited Feb. 5, 2025).

3100 W. Charleston Blvd., #208 Las Vegas, NV 89102 SJG STRANCH, JENNINGS & GARVEY PLLC 725-235-9750 lasvegas@stranchlaw.com

of its current and former employes in an Internet-accessible environment, had reason to be on guard for the exfiltration of the Private Information and Defendant's type of business had cause to be particularly on guard against such an attack.

62. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' Private Information could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

63. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted its employees' Social Security numbers and other sensitive data elements within the Private Information to protect against their publication and misuse in the event of a cyberattack.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

64. Plaintiff and members of the proposed Class have suffered injury from the misuse of their Sensitive Information that can be directly traced to Defendant.

65. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Sensitive Information is used;

b. The diminution in value of their Sensitive Information;

c. The compromise and continuing publication of their Sensitive Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Sensitive Information; and

h. The continued risk to their Sensitive Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Sensitive Information in its possession.

66. Stolen Sensitive Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII alone can be worth up to $1,000.00 depending on the type of information obtained.

67. The value of Plaintiff's and the Class's Sensitive Information on the black market is considerable. Stolen Sensitive Information trades on the black market for years, and criminals frequently post stolen Sensitive Information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

68. It can take victims years to spot identity theft, giving criminals plenty of time to use that information to commit acts of identity theft and fraud.

69. One such example of criminals using Sensitive Information for profit is the development of "Fullz" packages.

70. Cyber-criminals can cross-reference two sources of Sensitive Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

71. The development of "Fullz" packages means that stolen Sensitive Information from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Sensitive Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen Sensitive Information is being misused, and that such misuse is fairly traceable to the Data Breach.

72. Defendant disclosed the Sensitive Information of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Sensitive Information of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Sensitive Information.

73. Defendant's failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Sensitive Information and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

74. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Sensitive Information.

75. In 2016, the FTC updated its publication, Protecting Sensitive Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of Sensitive Information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

76. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

77. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

78. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

79. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Fails to Comply with Industry Standards

80. As noted above, experts studying cyber security routinely identify entities in possession of PII and PHI as being particularly vulnerable to cyberattacks because of the value of the Sensitive Information which they collect and maintain.

81. Several best practices have been identified that a minimum should be implemented by employers in possession of PII and PHI, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

82. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

83. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

84. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

85. Plaintiff brings this nationwide class action on behalf of herself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

86. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **All individuals whose Sensitive Information was accessed without authorization in the Data Breach, including all those who received a notice of the Data Breach.**

87. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

88. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

89. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

all members is impracticable. Upon information and belief, there are at least 1280 individuals[26] who were notified by Defendant of the Data Breach. Tens of thousands of individuals had their Sensitive Information compromised in this Data Breach. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

90. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the Sensitive Information of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the Sensitive Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the Sensitive Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Sensitive Information of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Sensitive Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Sensitive Information had been compromised;

[26] N. 5.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Sensitive Information of Plaintiff and Class Members;

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

91. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their Sensitive Information compromised as a result of the Data Breach, due to Defendant' misfeasance.

92. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

93. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff have suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

94. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

95. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

96. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

97. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

98. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure the Sensitive of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

99. Further, Defendant have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

100. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Sensitive Information;

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Sensitive Information;

c. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Sensitive Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Sensitive Information of Plaintiff and Class Members;

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT ONE

NEGLIGENCE

(On behalf of Plaintiff and the Class)

101. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

102. Defendant solicited, gathered, and stored the Sensitive Information of Plaintiff and the Class as part of the operation of its business and in order to gain profit.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

103. All Plaintiff and the Class Members entrusted their Sensitive Information to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their Sensitive Information for employment/business purposes only, and/or not disclose their Sensitive Information to unauthorized third parties.

104. Upon accepting and storing the Sensitive Information of Plaintiff and Class members, Defendant undertook and owed a duty to Plaintiff and Class members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so.

105. Defendant had full knowledge of the sensitivity of the Sensitive Information, the types of harm that Plaintiff and Class members could and would suffer if the Sensitive Information was wrongfully disclosed, and the importance of adequate security.

106. Plaintiff and Class members were the foreseeable victims of any inadequate safety and security practices on the part of Defendant. Plaintiff and the Class members had no ability to protect their Sensitive Information that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiff and the Class.

107. Defendant was well aware of the fact that cyber criminals routinely target large corporations through cyberattacks in an attempt to steal sensitive personal information.

108. Defendant owed Plaintiff and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

109. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures also have recognized the existence of a specific duty to reasonably safeguard Sensitive Information.

110. Defendant had duties to protect and safeguard the Sensitive Information of Plaintiff and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with Sensitive Information. Additional duties that Defendant owed Plaintiff and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, email accounts, protocols, policies, procedures and practices to ensure that Plaintiff's and Class members' Sensitive Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's and Class members' Sensitive Information in its possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its business email system, networks and servers; and

d. To promptly notify Plaintiff and Class members of any data breach, security incident, or intrusion that affected or may have affected their Sensitive Information.

111. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Sensitive Information that Plaintiff and the Class had entrusted to it.

112. Defendant breached its duty of care by failing to adequately protect Plaintiff's and Class members' Sensitive Information. Defendant breached its duties by, among other things:

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the Sensitive Information in its possession;

b. Failing to protect the Sensitive Information in its possession by using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees to avoid phishing emails;

d. Failing to use adequate email security systems, including industry standard SPAM filters, DMARC enforcement, and/or Sender Policy Framework enforcement to protect against phishing emails;

e. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Sensitive Information;

f. Failing to adequately train its employees to not store Sensitive Information longer than absolutely necessary for the specific purpose that it was sent or received;

g. Failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class's Sensitive Information;

h. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

i. Failing to promptly notify Plaintiff and Class members of the Data Breach that affected their Sensitive Information.

113. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

114. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

115. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Sensitive Information of Plaintiff and Class members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Sensitive Information of Plaintiff and Class members while it was within Defendant's possession and control.

116. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class members, Defendant prevented Plaintiff and Class members from taking meaningful, proactive steps toward securing their Sensitive Information and mitigating damages.

117. As a result of the Data Breach, Plaintiff and Class members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to fraudulent activity, closely monitoring bank account activity, and examining credit reports and statements sent from providers and their insurance companies.

118. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

119. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

120. In addition to its duties under common law, Defendant had additional duties imposed by statute and regulations, including the duties under the FTC Act. The harms which occurred as a result of Defendant's failure to observe these duties, including the loss of privacy, lost time and expense, and significant risk of identity theft are the types of harm that these statutes and regulations intended to prevent.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

121. Defendant violated these statutes when it engaged in the actions and omissions alleged herein, and Plaintiff's and Class members' injuries were a direct and proximate result of Defendant's violations of these statutes. Plaintiff therefore is entitled to the evidentiary presumptions for negligence *per se*.

122. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant owed a duty to Plaintiff and the Class to provide fair and adequate computer systems and data security to safeguard the Sensitive Information of Plaintiff and the Class.

123. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Sensitive Information. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

124. Defendant gathered and stored the Sensitive Information of Plaintiff and the Class as part of its business, which affect commerce.

125. Defendant violated the FTC Act by failing to use reasonable measures to protect the Sensitive Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

126. Defendant breached its duties to Plaintiff and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiff's and Class members' Sensitive Information, and by failing to provide prompt and specific notice without reasonable delay.

127. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

128. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

129. Defendant breached its duties to Plaintiff and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Sensitive Information.

130. Defendant breached its duties to Plaintiff and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiff and the Class.

131. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

132. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence.

133. Plaintiff and the Class have suffered injury and are entitled to actual and punitive damages in amounts to be proven at trial.

COUNT TWO
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

134. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

135. Plaintiff and Class Members either directly contracted with Defendant or Plaintiff and Class Members were the third-party beneficiaries of contracts with Defendant.

136. Plaintiff and Class Members (or their third-party agents) were required to provide their Sensitive Information to Defendant as a condition of receiving services provided by Defendant. Plaintiff and Class Members (or their third-party agents) provided their Sensitive Information to Defendant or its third-party agents in exchange for Defendant's services.

137. Plaintiff and Class Members (or their third-party agents) reasonably understood that a portion of the funds they paid would be used to pay for adequate cybersecurity measures.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

138. Plaintiff and Class Members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the Sensitive Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

139. Plaintiff and the Class Members (or their third-party agents) accepted Defendant's offers by disclosing their Sensitive Information to Defendant or its third-party agents in exchange for services.

140. In turn, and through internal policies, Defendant agreed to protect and not disclose the Sensitive Information to unauthorized persons.

141. In its Privacy Policy, Defendant represented that it had a legal duty to protect Plaintiff's and Class Member's Sensitive Information.

142. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class Members (or their third-party agents) with prompt and adequate notice of all unauthorized access and/or theft of their Sensitive Information.

143. After all, Plaintiff and Class Members (or their third-party agents) would not have entrusted their Sensitive Information to Defendant (or their third-party agents) in the absence of such an agreement with Defendant.

144. Plaintiff and the Class (or their third-party agents) fully performed their obligations under the implied contracts with Defendant.

145. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

146. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

147. Defendant materially breached the contracts it entered with Plaintiff and Class Members (or their third-party agents) by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic Sensitive Information that Defendant created, received, maintained, and transmitted.

148. In these and other ways, Defendant violated its duty of good faith and fair dealing.

149. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class Members' injuries (as detailed supra).

150. And, on information and belief, Plaintiff's Sensitive Information has already been published—or will be published imminently—by cybercriminals on the dark web.

151. Plaintiff and Class Members (or their third-party agents) performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

COUNT THREE
UNJUST ENRICHEMNT
(On behalf of Plaintiff and the Class)

152. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

153. Plaintiff and Class members (or their third-party agents) conferred a benefit upon Defendant. After all, Defendant benefitted from using their Sensitive Information to provide dental retail software services.

154. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members (or their third-party agents). And Defendant benefited from receiving Plaintiff's and Class members' Sensitive Information, as this was used to provide dental benefit services.

155. Plaintiff and Class members (or their third-party agents) reasonably understood that Defendant would use adequate cybersecurity measures to protect the Sensitive Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

156. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' Sensitive Information.

157. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

158. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class members' payment because Defendant failed to adequately protect their Sensitive Information.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

159. Plaintiff and Class members have no adequate remedy at law.

160. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT FOUR
Violation of the Nevada Consumer Fraud Act
Nev. Rev. Stat. § 41.600
(On Behalf of Plaintiff and the Class)

161. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

162. The Nevada Consumer Fraud Act, Nev. Rev. Stat. § 41.600 states in relevant part: "An action may be brough by any person who is a victim of consumer fraud."

163. As used in this section, "consumer fraud" means: . . . A deceptive trade practice defined in NRS 598.0915 to 598.0225, inclusive. Nev. Rev. Stat. § 41.600(1) & (2)(e).

164. In turn, Nev. Rev. Stat. § 598.0923(2) provides that "[a] person engages in a 'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly . . . [f]ails to disclose a material fact in connection with the sale or lease of goods or services." *Id.* Defendant violated this provision because it failed to disclose the material fact that its data security measures were inadequate to reasonably safeguard its customers' Sensitive Information. This is true because, among other things, Defendant was aware of the risks of cyberattacks such as the Data Breach. Defendant knew or should have known that that its data security measures were insufficient to guard against attacks such as the Data Breach. Defendant had knowledge of the facts that constituted the omission. Defendant could have and should have made a proper disclosure prior to providing services to customers by any other means reasonably calculated to inform customers of its inadequate data security measures.

165. Further, Nev. Rev. Stat. § 598.0923(3) provides that "[a] person engages in a

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

'deceptive trade practice' when in the course of his or her business or occupation he or she knowingly . . . [v]iolates a state or federal statute or regulation relating to the sale or lease of goods or services." *Id.* Defendant violated this provision for several reasons, each of which serves as an independent basis for violating Nev. Rev. Stat. § 598.0923(3).

166. First, Defendant breached its duty under Nev. Rev. Stat. § 603A.210, which requires any data collector "that maintains records which contain personal information" of Nevada residents to "implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, . . . use, modification or disclosure." *Id.* Defendant is a "data collector" as defined by Nev. Rev. Stat. § 603A.030. Defendant failed to implement such reasonable security measures, as shown by a system-wide breach of its computer systems during which a threat actor exfiltrated its clients' Sensitive Information. Defendant's violation of this statute was done knowingly for the purposes of Nev. Rev. Stat. § 598.0923(3) because Defendant knew or should have known that it would be a target of cyberattacks such as the Data Breach. Defendant knew or should have known that its data security measures were inadequate to protect against cyberattacks such as the Data Breach.

167. Second, Defendant violated Section 5 of the FTC Act, as alleged above. Defendant knew or should have known that its data security measures were inadequate, violated Section 5 of the FTC Act and failed to adhere to the FTC's data security guidance. This is true because Defendant was well aware that the casino industry is a frequent target of cyberattacks such as the Data Breach and the FTC has recommended various data security measures that companies such as Defendant could have implemented to mitigate the risk of a Data Breach. Defendant chose not to follow such guidance and knew or should have known that its data security measures were inadequate to guard against cyberattacks such as the Data Breach. Defendant had knowledge of the facts that constituted the violation. Defendant's violation of Section 5 of the FTC Act serves as a separate actional basis

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

for purposes of violating Nev. Rev. Stat. § 598.0923(3).

168. Defendant engaged in an unfair practice by engaging in conduct that is contrary to public policy, unscrupulous, and caused injury to Plaintiff and Class Members.

169. Plaintiff and members of the Class were denied a benefit conferred on them by the Nevada legislature.

170. As a direct and proximate result of the foregoing, Plaintiff and Class Members have suffered injuries including, but not limited to actual damages, and in being denied a benefit conferred on them by the Nevada legislature.

171. As a result of these violations, Plaintiff and Class Members are entitled to an award of actual damages, equitable injunctive relief requiring Defendant to implement adequate data security measures, as well as an award of reasonable attorney's fees and costs. Nev. Rev. Stat. § 41.600(3).

COUNT FIVE
DECLARATORY JUDGMENT
(On behalf of Plaintiff and the Class)

172. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

173. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary supplemental relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

174. In the fallout of the Data Breach, a controversy has arisen about Defendant's duty to use reasonable data security for the Sensitive Information it collects and maintains from employees and customers.

175. On information and belief, Defendant's actions were—and *still* are—inadequate and

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
725-235-9750
lasvegas@stranchlaw.com
STRANCH, JENNINGS & GARVEY PLLC

unreasonable. Plaintiff and Class Members continue to suffer injuries from the ongoing threat of fraud and identity theft due to Defendant's inadequate data security measures.

176. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring as follows:

a. Defendant owed and continues to owe a legal duty to use reasonable data security to secure the Sensitive Information entrusted to it;

b. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to protect the Sensitive Information entrusted to it from unauthorized access, use, and disclosure; and

c. Defendant's breaches of duties caused and continue to cause injuries to Plaintiff and Class Members.

177. The Court should also issue injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the Sensitive Information entrusted to it.

178. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injuries and lack an adequate legal remedy if Defendant experiences a second data breach. And if a second breach occurs, Plaintiff and Class Members will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full, and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted for out-of-pocket damages and other legally quantifiable and provable damages, cannot cover the full extent of Plaintiff's and Class Members' injuries.

179. If an injunction is not issued, the resulting hardship to Plaintiff and Class Members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

180. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class Members, and the public at large.

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
SJG STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual damages, restitution, attorney fees, expenses, costs, and such other and further relief as is just and proper.

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:

i. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

iii. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

iv. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of

Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

v. Ordering that Defendant cease transmitting Sensitive Information via unencrypted email;

vi. Ordering that Defendant cease storing Sensitive Information in email accounts;

vii. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

viii. Ordering that Defendant conduct regular database scanning and securing checks;

ix. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

x. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats faced as a result of the loss of financial and personal information to third parties, as well as the steps they must take to protect against such occurrences;

d. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;

3100 W. Charleston Blvd., #208
Las Vegas, NV 89102
STRANCH, JENNINGS & GARVEY PLLC
725-235-9750
lasvegas@stranchlaw.com

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

An award of such other and further relief as this Court may deem just and proper

JURY DEMAND

Plaintiff hereby demand that this matter be tried before a jury.

Dated: June 25, 2025

Respectfully Submitted,

/s/ Nathan R. Ring

Nathan R. Ring
Nevada State Bar No. 12078
STRANCH, JENNINGS & GARVEY, PLLC.
3100 W. Charleston Boulevard
Suite 208
Las Vegas, NV 89102
(725) 235-9750
nring@stranchlaw.com

Raina C. Borrelli, Esq.*
Samuel J. Strauss, Esq.*
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
raina@straussborrelli.com
sam@straussborrelli.com

* *Pro hac vice forthcoming*

Attorneys for Plaintiff and the Proposed Class